Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1 - 18. (Cancelled)

19. (Previously presented) A computer implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values (Q_i, G_i) verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i (for $i = 1, \ldots, m$) is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i (for $i = 1, \ldots, m$) is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, \ldots, p_f$, and g_i is a non-quadratic residue of the body of integers modulo n; and

using at least the private values $Q_1, Q_2, \ldots, Q_m$ in an authentication or in a signature method.

20. (Previously presented) The computer implemented process according to claim 19, further comprising:

receiving a commitment R from a demonstrator, the commitment R having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value computed such that: $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \ldots \times Q_m^{d_m} \bmod n$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \ldots \times G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

21. (Previously presented) The computer implemented process according to claim 19, further comprising:

receiving a commitment R from a demonstrator, the commitment R having a value computed using the Chinese remainder method from a series of commitment components R_j, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1, \ldots, f$, wherein $r_1, \ldots, r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times \ldots \times Q_{m,j}^{d_m} \bmod p_j$ for $j = 1, \ldots, f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, \ldots, m$ and $j = 1, \ldots, f$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \ldots \times G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

22. (Previously presented) The computer implemented process according to claim 19, further comprising:

receiving a token T from a demonstrator, the token T having a value such that $T = h(M,R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value such that: $D = r \times Q_1^{d_1} \times Q_2^{d_2} \times \ldots \times Q_m^{d_m} \bmod n$; and

determining that the message M is authentic if the response D has a value such that: $h\left(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \ldots \times G_m^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

23. (Previously presented) The computer implemented process according to claim 19, further comprising:

receiving a token T from a demonstrator, the token T having a value such that $T = h(M,R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed out of commitment components R_j by using the Chinese remainder method, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1, \ldots, f$, wherein $r_1, \ldots, r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times ... \times Q_{m,j}^{d_m} \bmod p_j$ for $j = 1, ..., f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, ..., m$ and $j = 1, ..., f$; and

determining that the message M is authentic if the response D has a value such that: $h(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n)$ is equal to the token T, wherein, for $i = 1, ..., m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

24. (Previously presented) The process according to claim 20, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, ..., m$.

25. (Previously presented) A process according to claim 19 for allowing a signatory to sign a message M, the method further comprising:

choosing m integers r_i randomly, wherein i is an integer between 1 and m;

computing commitments R_i having a value such that: $R_i = r_i^v \bmod n$ for $i = 1, ..., m$;

computing a token T having a value such that $T = h(M, R_1, R_2, ..., R_m)$, wherein h is a hash function producing a binary train consisting of m bits;

identifying the bits $d_1, d_2, ..., d_m$ of the token T; and

computing responses $D_i = r_i \times Q_i^{d_i} \bmod n$ for $i = 1, ..., m$.

26. (Currently amended) The process of claim 25, further comprising:

collecting the token T and the responses D_i for $i = 1, ..., m$; and

determining that the message M is authentic if the response D has a value such that:

$$\cancel{h\left(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times \ldots \times G_m^{\varepsilon_m d_m} \bmod n\right)}$$

$$\underline{h\left(M, D_1^v \times G_1^{\varepsilon_1 d_1} \bmod n, D_2^v \times G_2^{\varepsilon_2 d_2} \bmod n, \ldots, D_m^v \times G_m^{\varepsilon_m d_m} \bmod n\right)}$$

is equal to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

27. (Cancelled)

28. (Previously presented) A computer readable medium containing computer code programmed for execution on multiple threads, the computer code comprising:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of keys (Q_i, G_i) verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i (for $i = 1, \ldots, m$) is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i (for $i = 1, \ldots, m$) is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, \ldots, p_f$, and g_i is a non-quadratic residue of the body of integers modulo n; and

using at least the private values $Q_1, Q_2, \ldots, Q_m$ in an authentication or in a signature method.